# ITP 475
# Advanced Digital Forensics

## Amcache

# Overview

- Understanding the Amcache.hve
  - What is it?
  - How is data stored?
  - Forensic significance?
- Brief overview of RecentFileCache.bcf
- Amcache Structure
  - Version differences?
- Parsing Amcache files

# Background

- Amcache.hve stores information related to the Windows Application Experience and Compatibility feature inside a registry hive file
  - As a result, it contains data about applications that have been run
  - Official use is to track application compatibility issues
- First appeared in Windows 8 to replace the “RecentFileCache.bcf”, which was a similar structure in Windows 7

# What is it?

- It is a Registry hive containing critical information related to executed applications

# Forensic Significance

- Another indicator of program execution!
  - Unlike other artifacts such as UserAssist or RecentApps, it is not specifically user tied
- Traces of anti-forensic programs
- Traces of portable programs
- Traces of external storage devices
- Traces of malware executions

# Structure and Stored Information

- It’s just a Registry hive, we know the structure
- Stored information includes
  - Execution path
  - First executed time
  - Deleted time (if deleted)
  - First installation time
  - SHA1 Hashes!!!

# What does it track?

- Application name and file path
- Creation timestamp
- Does NOT record the run count of applications
  - Corroborate with other artifacts for constructing a comprehensive timeline

# Location

- <SystemRoot>\Windows\AppCompat\Programs\Amcache.hve

# Amcache Across Windows Versions

- Available on Windows 10, 8.1, and 8 by default
- Available on Windows 7 systems running the optional KB2952664 Windows Update or newer
  - Otherwise the RecentFileCache.bcf is in its place
- NOT available on Vista or XP
- Available on Windows Server 2019, 2016, 2012 R2, and 2012

# More Caveats…

- Different installed updates may result in a different Amcache structure
  - Microsoft has consistently changed the structure and behavior of the Amache between versions
  - The majority of the data remains the same between versions, the structure of the hive does not

# Windows 7 SP0 and SP1 "fresh" RecentFileCache.bcf

- <SystemRoot>\Windows\AppCompat\Programs\RecentFileCache.bcf
  - Application Experience service records the file names of executables
  - Temporary, the file is cleared when Application Experience ProgramDataUpdater task is run
  - The ProgramDataUpdater task runs at least once a day and knowing it clears the cache means the programs listed in the RecentFileCache.bcf file executed fairly recently

# Windows 7 SP0 and SP1 "fresh" RecentFileCache.bcf

- <SystemRoot>\Windows\AppCompat\Programs\AEINV_PREVIOUS.xml
- <SystemRoot>\Windows\AppCompat\Programs\AEINV_WER

# Forensic significance of the RecentFileCache.bcf

- Programs listed in the RecentFileCache.bcf indicate that
  - The program is fairly new to the system
    - Recall the cache is cleared daily
  - The program executed on the system
    - Recall the cache tracks applications to determine if they need shimming
  - The program executed on the system after the ProgramDataUpdater task was last run
    - Recall the ProgramDataUpdater task flushes the RecentFileCache.bcf daily

# Windows 10 1607 Updates to Amcache

- Major changes beginning with version 10.0.14913.1002 of the libraries
- What's new?
  - Application shortcuts
  - Device containers
  - Device interfaces
  - Device PnP information
  - Device driver binary informatin
  - Device driver package information

# New Amcache.hve Keys

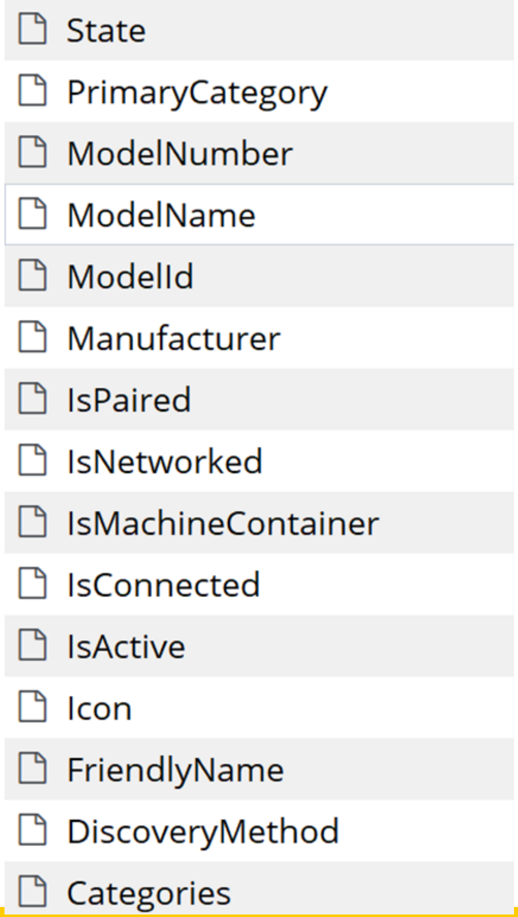
- InventoryDriverBinary
- InventoryDriverPackage
- DeviceCensus
- InventoryDeviceMediaClass
- InventoryDeviceContainer
- InventoryDevicePnp
- InventoryApplication
- InventoryApplicationFile

# Root\InventoryApplicationShortcut Key

- Contains information about the target of the LNK file (often truncated)
- Each subkey contains a single value to a shortcut

# Root\InventoryDeviceContainer Key

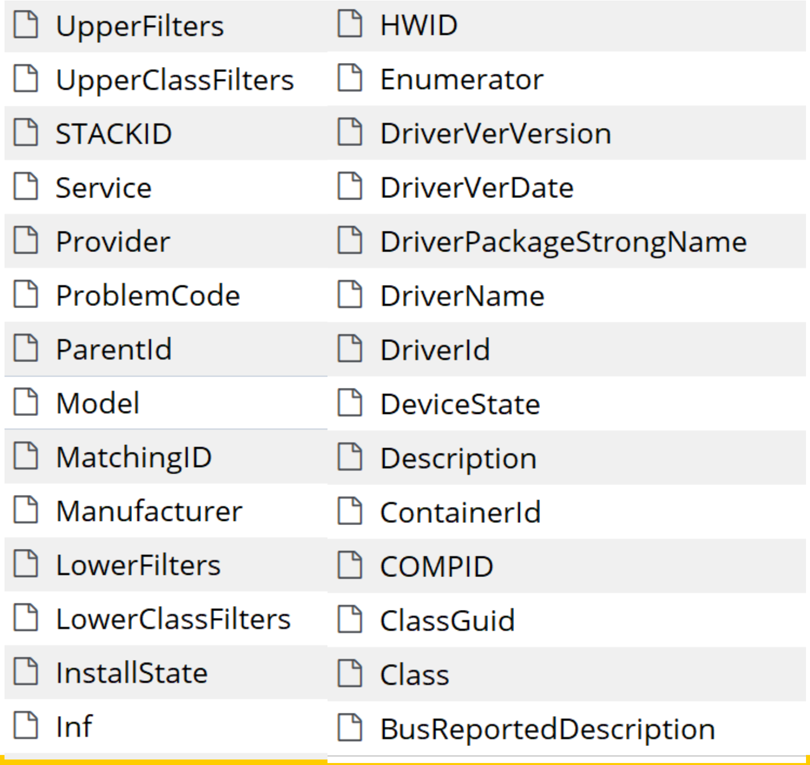
- Tracks devices such as Bluetooth, printers, audio, storage, etc.
- Each key has 15 values



State
PrimaryCategory
ModelNumber
ModelName
ModelId
Manufacturer
IsPaired
IsNetworked
IsMachineContainer
IsConnected
IsActive
Icon
FriendlyName
DiscoveryMethod
Categories

# Root\InventoryDevicePnp Key

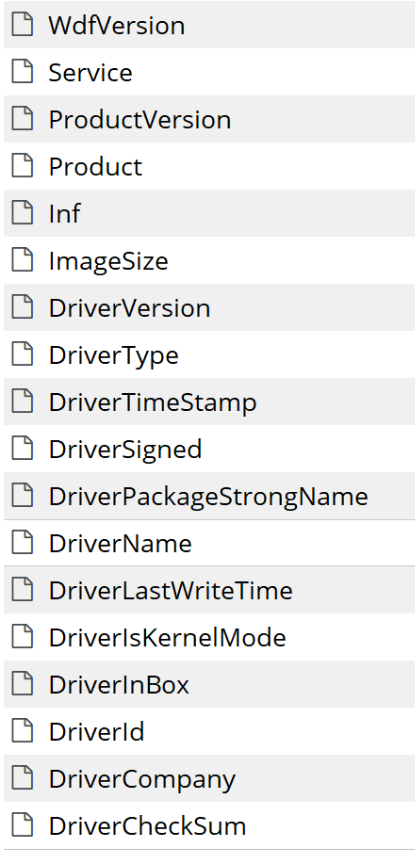
- Plug and play devices
- Each key has 28 values



UpperFilters
UpperClassFilters
STACKID
Service
Provider
ProblemCode
ParentId
Model
MatchingID
Manufacturer
LowerFilters
LowerClassFilters
InstallState
Inf
HWID
Enumerator
DriverVerVersion
DriverVerDate
DriverPackageStrongName
DriverName
DriverId
DeviceState
Description
ContainerId
COMPID
ClassGuid
Class
BusReportedDescription

# Root\InventoryDriverBinary Key

- Subkeys refer to the full path of a driver
- Each key has 18 values
- Notable keys include:
  - DriverSigned
  - DriverIsKernelMode
  - DriverTimeStamp
  - DriverLastWriteTime



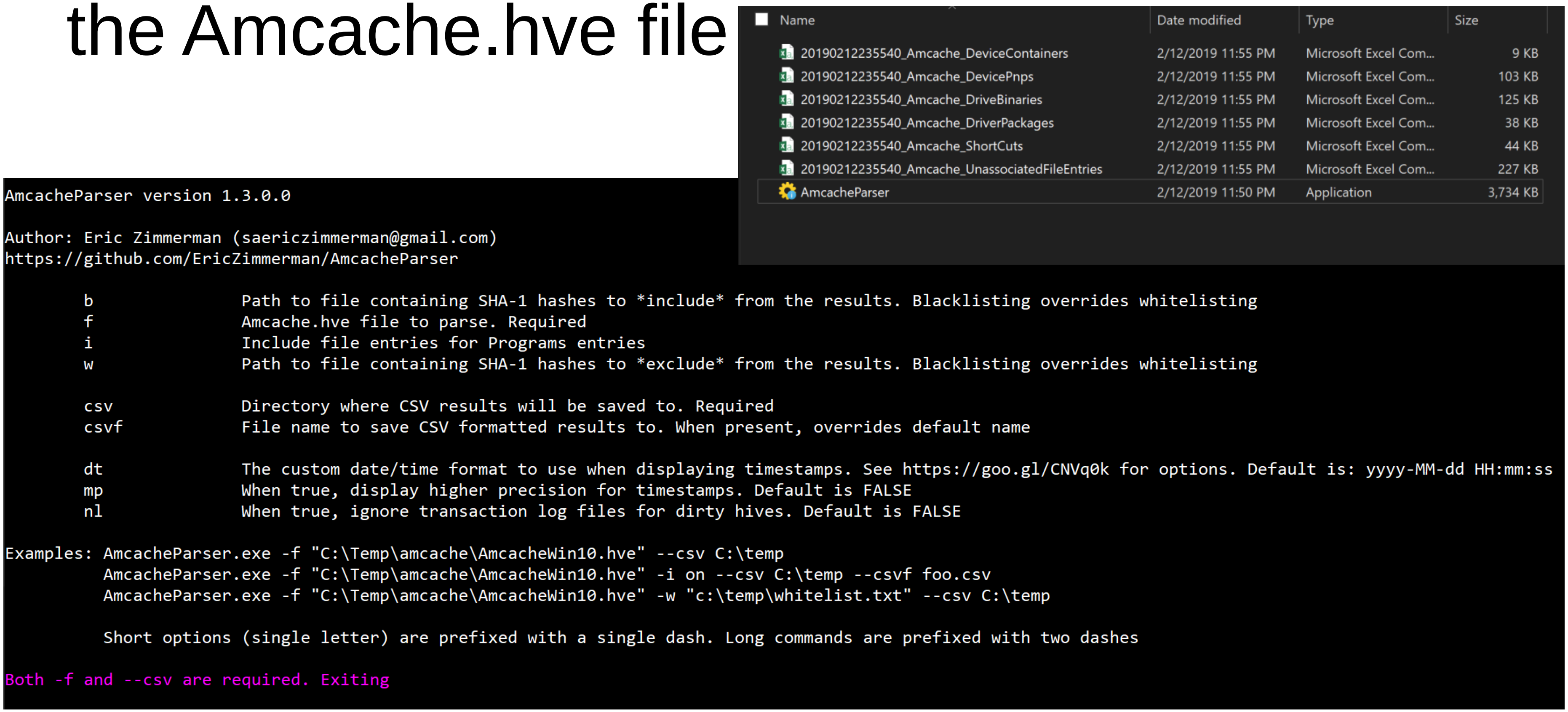
WdfVersion
Service
ProductVersion
Product
Inf
ImageSize
DriverVersion
DriverType
DriverTimeStamp
DriverSigned
DriverPackageStrongName
DriverName
DriverLastWriteTime
DriverIsKernelMode
DriverInBox
DriverId
DriverCompany
DriverCheckSum

# Parsing the Amcache

- It is a registry structured file, EnCase can “parse” out the structure (ie. View the file structure)
- Plugin for Harlan Carvey’s RegRipper
  - https://github.com/keydet89/RegRipper2.8
- Eric Zimmerman’s Parser
  - https://ericzimmerman.github.io/#!index.md
  - Usage here https://binaryforay.blogspot.com/2015/07/amcacheparser-reducing-noise-finding.html
  - Works on the new format of the Amcache
- Will Ballethin’s Parser
  - https://github.com/williballenthin/python-registry/blob/master/samples/amcache.py
- Yogesh Khatri’s Enscript
  - http://www.swiftforensics.com/p/downloads.html
- Or write your own as a pet project ;)

# Parsing the Amcache (cont.)

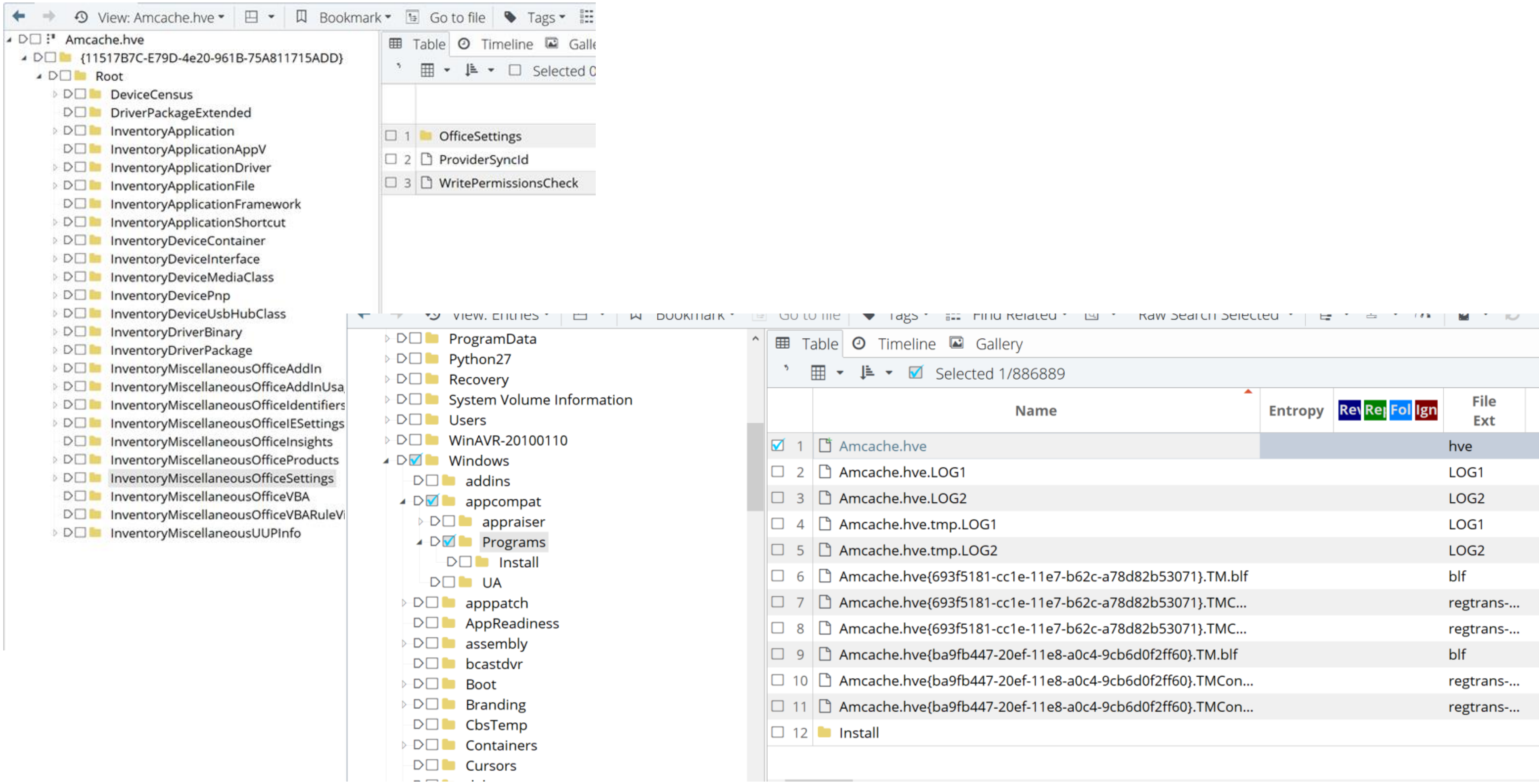
- Zimmerman’s command line tool that takes in the Amcache.hve file



| Name | Date modified | Type | Size |
|---|---|---|---|
| 20190212235540_Amcache_DeviceContainers | 2/12/2019 11:55 PM | Microsoft Excel Com... | 9 KB |
| 20190212235540_Amcache_DevicePnps | 2/12/2019 11:55 PM | Microsoft Excel Com... | 103 KB |
| 20190212235540_Amcache_DriveBinaries | 2/12/2019 11:55 PM | Microsoft Excel Com... | 125 KB |
| 20190212235540_Amcache_DriverPackages | 2/12/2019 11:55 PM | Microsoft Excel Com... | 38 KB |
| 20190212235540_Amcache_ShortCuts | 2/12/2019 11:55 PM | Microsoft Excel Com... | 44 KB |
| 20190212235540_Amcache_UnassociatedFileEntries | 2/12/2019 11:55 PM | Microsoft Excel Com... | 227 KB |
| AmcacheParser | 2/12/2019 11:50 PM | Application | 3,734 KB |

```
AmcacheParser version 1.3.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

        b               Path to file containing SHA-1 hashes to *include* from the results. Blacklisting overrides whitelisting
        f               Amcache.hve file to parse. Required
        i               Include file entries for Programs entries
        w               Path to file containing SHA-1 hashes to *exclude* from the results. Blacklisting overrides whitelisting

        csv             Directory where CSV results will be saved to. Required
        csvf            File name to save CSV formatted results to. When present, overrides default name

        dt              The custom date/time format to use when displaying timestamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
        mp              When true, display higher precision for timestamps. Default is FALSE
        nl              When true, ignore transaction log files for dirty hives. Default is FALSE

Examples: AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" --csv C:\temp
          AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -i on --csv C:\temp --csvf foo.csv
          AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -w "c:\temp\whitelist.txt" --csv C:\temp

          Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Both -f and --csv are required. Exiting
```

# Viewing in EnCase



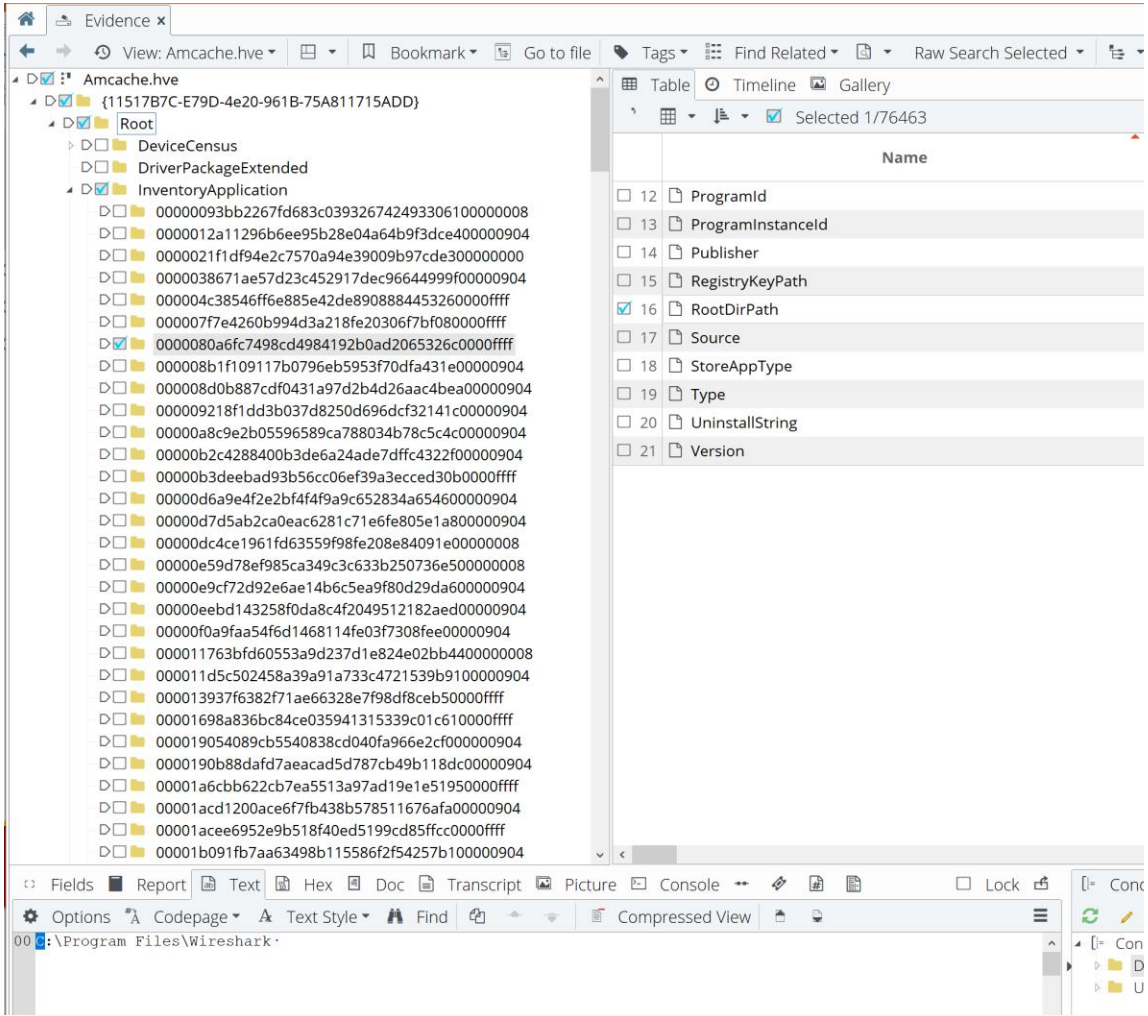
```
Amcache.hve
  {11517B7C-E79D-4e20-961B-75A811715ADD}
    Root
      DeviceCensus
      DriverPackageExtended
      InventoryApplication
      InventoryApplicationAppV
      InventoryApplicationDriver
      InventoryApplicationFile
      InventoryApplicationFramework
      InventoryApplicationShortcut
      InventoryDeviceContainer
      InventoryDeviceInterface
      InventoryDeviceMediaClass
      InventoryDevicePnp
      InventoryDeviceUsbHubClass
      InventoryDriverBinary
      InventoryDriverPackage
      InventoryMiscellaneousOfficeAddIn
      InventoryMiscellaneousOfficeAddInUsa
      InventoryMiscellaneousOfficeIdentifiers
      InventoryMiscellaneousOfficeIESettings
      InventoryMiscellaneousOfficeInsights
      InventoryMiscellaneousOfficeProducts
      InventoryMiscellaneousOfficeSettings
      InventoryMiscellaneousOfficeVBA
      InventoryMiscellaneousOfficeVBARuleVi
      InventoryMiscellaneousUUPInfo
```

| | | |
|---|---|---|
| □ | 1 | OfficeSettings |
| □ | 2 | ProviderSyncId |
| □ | 3 | WritePermissionsCheck |

```
ProgramData
Python27
Recovery
System Volume Information
Users
WinAVR-20100110
Windows
  addins
  appcompat
    appraiser
    Programs
      Install
    UA
  apppatch
  AppReadiness
  assembly
  bcastdvr
  Boot
  Branding
  CbsTemp
  Containers
  Cursors
```

| | | Name | Entropy | Rev | Rep | Fol | Ign | File Ext |
|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | Amcache.hve | | | | | | hve |
| □ | 2 | Amcache.hve.LOG1 | | | | | | LOG1 |
| □ | 3 | Amcache.hve.LOG2 | | | | | | LOG2 |
| □ | 4 | Amcache.hve.tmp.LOG1 | | | | | | LOG1 |
| □ | 5 | Amcache.hve.tmp.LOG2 | | | | | | LOG2 |
| □ | 6 | Amcache.hve{693f5181-cc1e-11e7-b62c-a78d82b53071}.TM.blf | | | | | | blf |
| □ | 7 | Amcache.hve{693f5181-cc1e-11e7-b62c-a78d82b53071}.TMC... | | | | | | regtrans-... |
| □ | 8 | Amcache.hve{693f5181-cc1e-11e7-b62c-a78d82b53071}.TMC... | | | | | | regtrans-... |
| □ | 9 | Amcache.hve{ba9fb447-20ef-11e8-a0c4-9cb6d0f2ff60}.TM.blf | | | | | | blf |
| □ | 10 | Amcache.hve{ba9fb447-20ef-11e8-a0c4-9cb6d0f2ff60}.TMCon... | | | | | | regtrans-... |
| □ | 11 | Amcache.hve{ba9fb447-20ef-11e8-a0c4-9cb6d0f2ff60}.TMCon... | | | | | | regtrans-... |
| □ | 12 | Install | | | | | | |

# Viewing in EnCase (cont.)

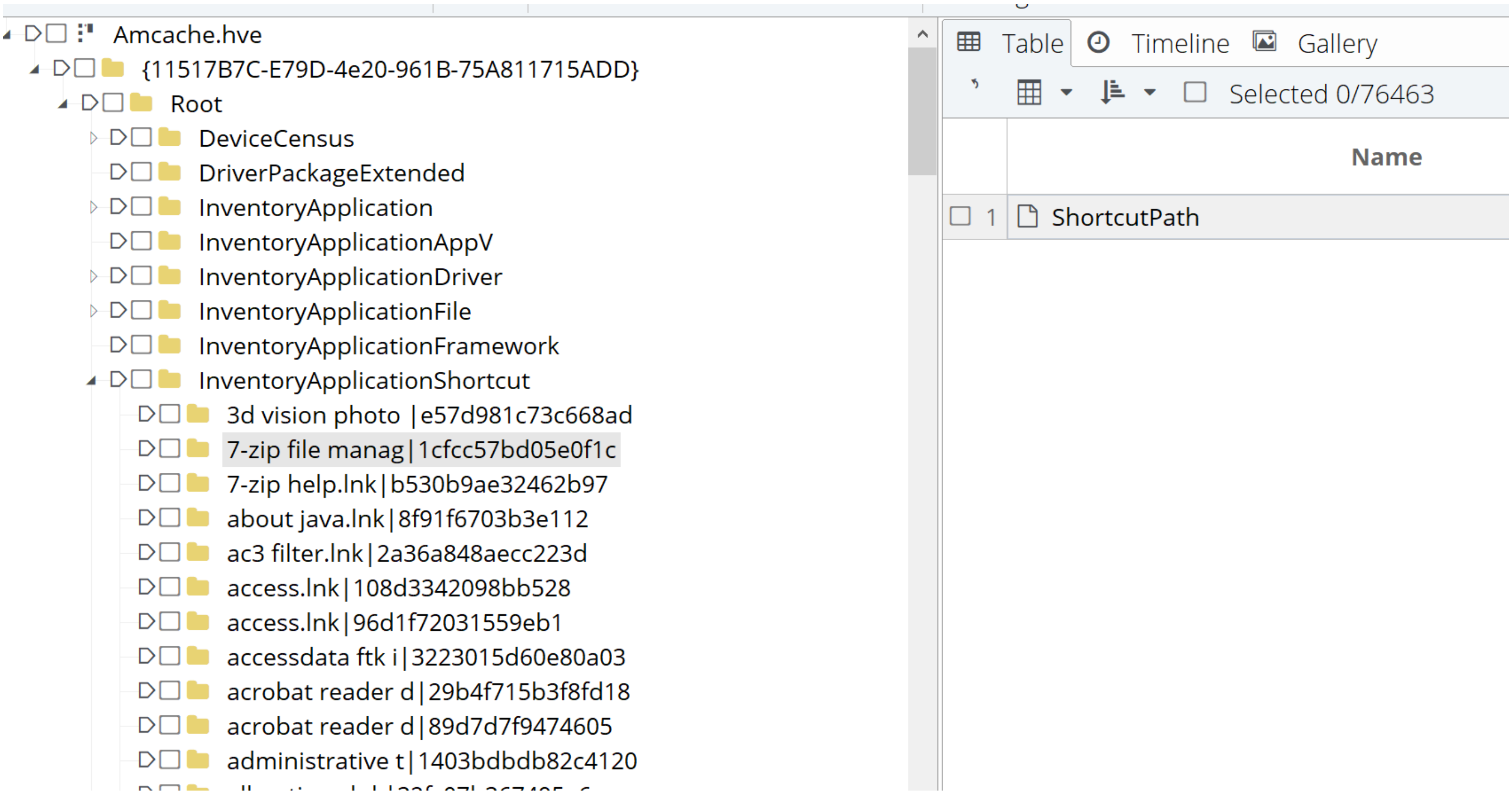


```
Amcache.hve
  {11517B7C-E79D-4e20-961B-75A811715ADD}
    Root
      DeviceCensus
      DriverPackageExtended
      InventoryApplication
        00000093bb2267fd683c0393267424933061000000008
        0000012a11296b6ee95b28e04a64b9f3dce400000904
        0000021f1df94e2c7570a94e39009b97cde300000000
        0000038671ae57d23c452917dec96644999f00000904
        000004c38546ff6e885e42de8908884453260000ffff
        000007f7e4260b994d3a218fe20306f7bf080000ffff
        0000080a6fc7498cd4984192b0ad2065326c0000ffff
        000008b1f109117b0796eb5953f70dfa431e00000904
        000008d0b887cdf0431a97d2b4d26aac4bea00000904
        000009218f1dd3b037d8250d696dcf32141c00000904
        00000a8c9e2b05596589ca788034b78c5c4c00000904
        00000b2c4288400b3de6a24ade7dffc4322f00000904
        00000b3deebad93b56cc06ef39a3ecced30b0000ffff
        00000d6a9e4f2e2bf4f4f9a9c652834a654600000904
        00000d7d5ab2ca0eac6281c71e6fe805e1a800000904
        00000dc4ce1961fd63559f98fe208e84091e00000008
        00000e59d78ef985ca349c3c633b250736e500000008
        00000e9cf72d92e6ae14b6c5ea9f80d29da600000904
        00000eebd143258f0da8c4f2049512182aed00000904
        00000f0a9faa54f6d1468114fe03f7308fee00000904
        000011763bfd60553a9d237d1e824e02bb4400000008
        000011d5c502458a39a91a733c4721539b9100000904
        000013937f6382f71ae66328e7f98df8ceb50000ffff
        00001698a836bc84ce035941315339c01c610000ffff
        000019054089cb5540838cd040fa966e2cf000000904
        0000190b88dafd7aeacad5d787cb49b118dc00000904
        00001a6cbb622cb7ea5513a97ad19e1e51950000ffff
        00001acd1200ace6f7fb438b578511676afa00000904
        00001acee6952e9b518f40ed5199cd85ffcc0000ffff
        00001b091fb7aa63498b115586f2f54257b100000904
```

|  |  | Name |
|---|---|---|
| ☐ | 12 | ProgramId |
| ☐ | 13 | ProgramInstanceId |
| ☐ | 14 | Publisher |
| ☐ | 15 | RegistryKeyPath |
| ☑ | 16 | RootDirPath |
| ☐ | 17 | Source |
| ☐ | 18 | StoreAppType |
| ☐ | 19 | Type |
| ☐ | 20 | UninstallString |
| ☐ | 21 | Version |

```
00 C:\Program Files\Wireshark·
```

# Viewing in EnCase (cont.)



- Amcache.hve
  - {11517B7C-E79D-4e20-961B-75A811715ADD}
    - Root
      - DeviceCensus
      - DriverPackageExtended
      - InventoryApplication
      - InventoryApplicationAppV
      - InventoryApplicationDriver
      - InventoryApplicationFile
      - InventoryApplicationFramework
      - InventoryApplicationShortcut
        - 3d vision photo |e57d981c73c668ad
        - 7-zip file manag|1cfcc57bd05e0f1c
        - 7-zip help.lnk|b530b9ae32462b97
        - about java.lnk|8f91f6703b3e112
        - ac3 filter.lnk|2a36a848aecc223d
        - access.lnk|108d3342098bb528
        - access.lnk|96d1f72031559eb1
        - accessdata ftk i|3223015d60e80a03
        - acrobat reader d|29b4f715b3f8fd18
        - acrobat reader d|89d7d7f9474605
        - administrative t|1403bdbdb82c4120

Selected 0/76463

| | Name |
|---|---|
| □ 1 | ShortcutPath |

# Conclusion

- The behavior of the Amache is dependent on the versions of the libraries, not by the OS version of the system
  - Ie. Investigating an older system that could have gone under several upgrades
  - Microsoft changed the structure of the Amcache over time
  - Some older parsers might not recognize the newer formats

# Links and references

- https://www.researchgate.net/publication/317258237_Leveraging_the_Windows_Amcachehve_File_in_Forensic_Investigations
- http://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-analysis_amcache.pdf
- https://binaryforay.blogspot.com/2017/10/amcache-still-rules-everything-around.html